AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A communication system in which a device and a client communicate data with each other through a network,

wherein said device comprises:

a first storage device which stores a root certificate including a public key paired with a private key and being signed with the private key;

a certificate creator which creates, when a connection for communication is requested by said client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to sign the root certificate; and

a communication device which transmits the second certificate created by said certificate creator to said client; and

wherein said client comprises:

a second storage device which has stored therein, before the connection for communication is requested to said device, the root certificate stored in said first storage device; and

a verifier which verifies the signature of the second certificate received from said device with the root certificate stored in said second storage device.

2. (Original) The communication system according to claim 1, wherein said device is a printer.

3. (Original) The communication system according to claim 1, wherein said device is a multifunctional peripheral.

4. (Original) The communication system according to claim 1, wherein said client is a personal computer.

5. (Original) The communication system according to claim 1, wherein said second storage device is a hard disk drive.

6. (Original) The communication system according to claim 1, wherein said second storage device is a read-only memory.

7. (Currently Amended) A communication method for a communication system in which a device and a client communicate data with each other through a network,

wherein the device holds a root certificate including a public key paired with a private key and being signed with the private key;

the client installs the root certificate which is held in the device and which includes the public key, prior to the client requesting a connection for communication to the device;

the device creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to sign the root certificate when data is sent to the client;

the device sends the second certificate to the client; and

the client verifies the signature of the second certificate received from the device with the installed root certificate.

8. (Previously Presented) The method according to claim 7, wherein the device further holds at least one intermediate certificate for one or more certificate authorities existing in a hierarchical order up to a root certificate authority;

the client installs the at least one intermediate certificate in addition to the root certificate;

the device sends the second certificate to the client; and

the client verifies the signature of the second certificate received from the device with the at least one intermediate certificate installed therein, and verifies the signature of the at least one intermediate certificate received from the device with the root certificate installed therein.

9. (Previously Presented) The method according to claim 7, wherein when the client installs the root certificate, the client requests the root certificate from the device when a printer driver from the device is installed in the client, receives the root certificate from the device, converts the received root certificate to a

predetermined format when the root certificate is received, and installs the converted root certificate.

10. (Previously Presented) The method according to claim 7, wherein when the client installs the root certificate, the installation is performed after the root certificate is confirmed by a user.

11. (Previously Presented) The method according to claim 7, wherein the device has a print function, and the client installs the root certificate after a printer driver from the device is installed in the client.

12. (Previously Presented) The method according to claim 7, wherein the data is communicated according to the security sockets layer (SSL) protocol.

13-16. (Cancelled)

17. (Currently Amended) A device to be used in a communication system in which the device and a client communicate with each other through a network, the device sends information to the client, and the client uses the information to communicate with the device, the device comprising:

a first storage device which stores a pair of a public key and a private key;

a second storage device which stores a root certificate signed with the private key;

a certificate creator which creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to sign the root certificate; and

an interface which sends the information as well as the root certificate including the public key to the client through the network before the connection for communication is requested to the device, and sends, after the root certificate stored in said second storage device is installed in the client, the second certificate to the client for verification of the information sent from the device.

18. (Previously Presented) The device according to claim 17, wherein the device is a device which functions as a printer.

19. (Previously Presented) The device according to claim 17, wherein the information is a printer driver.

20. (Previously Presented) The communication system according to claim 1, wherein the root certificate stored in said first storage device is stored in said second storage device prior to the transmission of the second certificate from said communication device.

21. (Cancelled)

22. (Previously Presented) The communication system according to claim 1, wherein said verifier is operable to verify the signature of the second certificate by decrypting the public key of the root certificate stored in said second storage device to obtain a first hash value, calculating a second hash value of the second certificate received from said device, and comparing the first and second hash values to determine if they are equal to each other.

23. (Previously Presented) The method according to claim 7, wherein the device sends the second certificate to the client after the root certificate is installed in the client.

24. (Previously Presented) The method according to claim 8, wherein the client installs the at least one intermediate certificate prior to receiving the second certificate from the device.

25-27. (Cancelled)

28. (New) The communication system according to claim 1, wherein:

the second storage device of said client has stored therein, before the connection for communication is requested to said device, the public key of the root certificate stored in said first storage device; and

the verifier verifies the signature of the second certificate received from said device by decrypting the second certificate with the public key of the root certificate stored in said second storage device.

29. (New) The communication method according to claim 7, wherein:

the client stores the public key of the installed root certificate, prior to the client requesting the connection for communication to the device; and

the client verifies the signature of the second certificate received from the device by decrypting the second certificate with the public key of the root certificate stored in the client.

30. (New) The device according to claim 17, further comprising:

a root certificate creator which creates the root certificate.

31. (New) A computer-readable recording medium having a computer program recorded thereon for causing a computing device, which is communicatively coupled to the computer-readable recording medium and which is configured to communicate with a client through a network to send information to the client, which uses the information to communicate with the computing device, to perform operations comprising:

storing a pair of a public key and a private key;

storing a root certificate signed with the private key;

sending the information and the root certificate including the public key to the client, before a request for communication is requested by the client;

creating, when the connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to sign the root certificate; and

sending, after the root certificate has been installed in the client, the created second certificate to the client for verification of the information sent from the computing device.

32. (New) The computer-readable recording medium according to claim 31, wherein the computing device is a device which functions as a printer.

33. (New) The computer-readable recording medium according to claim 31, wherein the information is a printer driver.